

Independence policy for certifications

Public edition, October 2026. Identical to the working document except that references to specific audit runs, datasets under private notice and their results are held back until November 10, 2026.

Plumblin Grader both finds weak tests (audits), writes stronger ones (repair), and certifies releases (Plumblin Verified). Selling repairs and then certifying the repaired release is a conflict of interest. These rules keep a certificate's result independent of any repair work.

1. **A certificate always rests on a fresh audit.** The certification audit is a new run, on a fresh random sample drawn after the release is final, with a new seed. It does not reuse the repair run's wrong patches, checks or candidates as its only attacks. Patches already known to the repair run may be included as extra attacks, never as a substitute for a new search. **A certificate is never issued by a run that did repair work:** the run that wrote or verified any of the release's tests (`plumblin-grader repair`, or a re-attack of those repairs) cannot be the certification audit. The certification record names both, and `plumblin-grader verified check` fails it when they are the same run.
2. **The certification audit uses the wider search.** Requirement-by-requirement and hole-pattern attacks, written by two attacker models from different companies, and the certificate reports the union estimate of holes the searches missed beside the confirmed count. One standard audit can miss most of the holes a wider search finds, so a certificate resting on one search would claim more than it tested.
3. **Disclosure.** If Plumblin Grader wrote or verified any tests in the certified release, the certificate says so, with the number of tasks involved.
4. **No outcome-based fees for certification.** A certification is priced per release, fixed before the audit starts. The fee never depends on whether the release passes.
5. **The method is fixed before the audit.** The certificate cites the method version (`docs/method.md`) and the run manifest. The method is not changed mid-audit for that release.
6. **Human sample.** Before any certificate is issued, a human reviewer who did not run the audit must review a random sample of findings with hidden controls, and their agreement is printed on the certificate. No certificate has been issued, and no such review has been done yet.
7. **Failed is published as failed.** A release that does not meet the criteria does not receive a certificate. The client may withhold the result, but Plumblin Grader never issues a softened or partial certificate.
8. **Records.** Every certificate's run directory, manifest and evidence bundle are kept for at least three years, so any certificate can be re-checked.

Findings reports (audits that are not certifications) are not bound by rules 1, 2, 4 and 6, but they always state their method version and that shares are floors.